NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Releases from 2 dams near Jamestown unprecedented. The U.S. Army Corps of Engineers said September 6 the amount of water that will pass through Jamestown, North Dakota, on the James River in 2011 is unprecedented. The Corps told the Jamestown Sun that releases from the Pipestem and Jamestown could reach 900,000 acre feet. The 2009 flows totaled about 530,000 acre feet. In some dry years, the dams had releases of nearly zero. Source: http://www.valleynewslive.com/story/15399076/releases-from-2-dams-near-jamestown-unprecedented

Regional

(South Dakota) **Arson spree probed.** Four fires that started late September 5 and early September 6 in central Sioux Falls, South Dakota are thought to be the work of arsonists, officials said. Three fires were reported in a garage, a shed, and a dumpster, with a trailer fire reported shortly after 9 a.m., that fire officials said is connected to the others. The fires were reported beginning at 11 p.m. September 5, and as of the afternoon of September 6, police said they had no suspects. A fire inspector and investigator with Sioux Falls Fire Rescue said the behavior of the fires and the pattern and location of them suggests they were all done by the same person or persons, and that they were set deliberately. Source: http://www.argusleader.com/article/20110907/NEWS/109070309/Arson-spree-probed

National

Nearly 100,000 told to flee Northeast flooding. Nearly 100,000 people from New York to Maryland were ordered to flee the rising Susquehanna River September 8 as the remnants of Tropical Storm Lee dumped more rain across the Northeast, closing major highways, and socking areas still recovering from Hurricane Irene. At Binghamton, New York, the wide river broke a flood record and flowed over retaining walls as more than 8 inches of rain fell in some areas. Road closures effectively sealed the city off to outside traffic as emergency responders scrambled to evacuate holdouts who didn't heed warnings to leave. Most of the people ordered to evacuate were about 80 miles downstream in Wilkes-Barre, Pennsylvania, where the river was projected to crest later Thursday at 41 feet — the same height as the levee system, officials said. Residents were ordered to leave by 4 p.m. In Port Deposit, Maryland, rising water levels at the Conowingo Dam forced officials to open the floodgates and order the evacuation of most of the town's 1,000 residents. There was also flooding upstream from Binghamton in Oneonta, New York. Roads and highways closed around the region, including sections of New York's Interstate 88, which follows the Susquehanna's path. In Philadelphia, flooding and a rock slide closed the eastbound lanes of the Schuylkill Expressway, a major artery into the city, and it could take hours for the road to reopen. The high waters were being blamed for the partial collapse of the Slabtown Bridge in Montoursville, Pennsylvania. A bridge spanning the Delaware River between New Hope, Pennsylvania, and Lambertville, New Jersey, closed September 8 as flood waters carried debris downriver. New York's Thruway Authority expected to close a 105-mile stretch of its busiest east-west highway, Interstate 90, because the Mohawk River had overflowed its banks in some areas. Wet weather followed by Hurricane Irene and its remnants have saturated the soil across the Northeast, leaving water no place to

go but into already swollen creeks and rivers. The National Weather Service predicted 4 to 10 inches of rain across the mid-Atlantic and Northeast through September 8. At least nine deaths have been blamed on Lee and its aftermath. Source: http://today.msnbc.msn.com/id/44436279/ns/weather/#.TmjAgexQhDg

INTERNATIONAL

Al Qaeda stockpiling chemical weapons. The ouster of Libyan leader's has provided an opportunity for al Qa'ida and other militant groups to stockpile large amounts of weapons, including chemical and biological weapons, the U.S. President's chief counter-terrorism adviser said recently. "We have indications that individuals of various stripes are looking to Libya and seeing it as an arms bazaar," said the assistant to the President for homeland security and counter-terrorism. "We are concerned about the potential for certain weapons to get into the hands of terrorists," he said. Libya's leader is also known to have accumulated a large stockpile of mustard gas. Recently seized documents suggest that in its final hours, his regime shipped large numbers of gas masks and chemical-protection suits to bases of support, according to the Christian Science Monitor. Human Rights Watch has said there were 20,000 surface-to-air missiles in Libya, and many of those are now missing. Source: http://economictimes.indiatimes.com/articleshow/9925915.cms

ConocoPhillips struggling with China oil spill. The oil spills from offshore wells operated by ConocoPhillips in China's Bohai Bay are posing political and technical challenges for the oil company far messier than the crude and drilling mud seeping from the seabed. The company said September 5 it had complied with a government order to suspend all drilling, water injection and production at the affected Penglai 19-3 oil field, one of China's biggest. Operations were stopped at 180 producing wells and 51 injecting wells, for a total of 231 wells, said a statement by Texas-based ConocoPhillips, which operates the field in a venture with state-owned China National Offshore Oil Corp. (CNOOC), which owns 51 percent of the venture, said the suspension of production in Penglai 19-3 would reduce output by 40,000 barrels a day, in addition to the 22,000 barrels a day lost with the shutdown of the two wells where the spills occurred. The spills began in early June and have unleashed a flood of criticism inside China over how ConocoPhillips has handled the cleanup. China's state oceanic administration rejected the company's assertion it met an August 31 deadline to completely clear up damage, and prevent further seeps. ConocoPhillips said September 5 that divers were continuing to search the ocean floor, and that remote-controlled robots were taking seabed samples. It said it was working with CNOOC on a plan to reduce pressure in the oil reservoir, and was preparing a revised environmental impact report. Source: http://www.google.com/hostednews/ap/article/ALeqM5j9oS2OX7c8kuBbkeeow_XA1WEI8Q?docId=b597749655254188a9b4bf3ccefa9da8

BANKING AND FINANCE INDUSTRY

Financial services company impersonated in malware spreading campaign. The Automated Clearing House (ACH), a financial service offered by the U.S. electronic payments association

National Automated Clearing House Association (NACHA), was impersonated in a campaign of spam messages sent out to unsuspecting users with the purpose of spreading malware. The samples investigated by MalwareCity seemed to be sent from a legitimate NACHA e-mail account. This specific message, named "ACH Transfer Review," informs the victim a transaction has failed and that she must review the input data for the payment. She then must fill the application form attached to the e-mail. The attachment is represented by a zip file that contains what seems to be a .pdf document that must be reviewed by the recipient. The .pdf file is actually an executable that installs a downloader on the soon-to-be infected computer. The downloader's purpose is to get other malware from the Web, and onto the computer. A few moments later, the Zeus bot, also known as Trojan(dot)Generic.6152125, is installed on the machine, closely monitoring all electronic financial transactions and sending out username and password information. The routing details from the message appear to come from a domain called "digitalskys.com", the Web site of a wireless solutions company, likely used by the cybercriminals to mask their true identity. Source: http://news.softpedia.com/news/Financial-Services-Company-Impersonated-in-Malware-Spreading-Campaign-220765.shtml

FBI releases bank crime statistics for second quarter of 2011. During the second quarter of 2011, there were 1,023 reported violations of the Federal Bank Robbery and Incidental Crimes Statue, a decrease from the 1,146 reported violations in the same quarter of 2010. According to statistics released September 7 by the FBI, there were 1,007 robberies, 15 burglaries, one larceny, and two extortions of financial institutions reported between April 1 and June 30. Source: http://www.fbi.gov/news/pressrel/press-releases/fbi-releases-bank-crime-statistics-for-second-quarter-of-2011

New financial malware attacks global financial institutions. Trusteer warned September 7 that a second non-financial malware variant called Shylock has been retrofitted with fraud capabilities and is abusing its large installed base of infected machines to attack global financial institutions. Unlike the non-financial malware Ramnit that turned into a fraud platform, Shylock does not incorporate tactics from the zeus trojan. It appears criminals have custom developed financial fraud capabilities for Shylock. Shylock uses unique mechanisms not found in other financial malware toolkits, including: an improved method for injecting code into additional browser processes to take control of the victim's computer; a better evasion technique to prevent malware scanners from detecting its presence; and a sophisticated watchdog service that allows it to resist removal attempts and restore operations. "As with all financial fraud toolkits, Shylock's detection rate among anti-malware solutions and fraud detection systems is extremely low," Trusteer's chief technology officer said. Source: http://www.net-security.org/malware_news.php?id=1830

Internet clothing seller charged with wire fraud. The owner of a defunct online clothing retail operation was arrested and charged September 2 with wire fraud for allegedly overcharging customers by more than $5 million. The owner of New York-based Classic Closeouts allegedly used customer credit and debit card numbers on file to charge accounts multiple times for items customers did not order, the U.S. Department of Justice (DOJ) said in a press release. Between June and December 2008, the operation charged customers for unordered items more

than 70,000 times, the DOJ said. In some cases, the same card was charged "multiple" times over many weeks, the agency said. The charges ranged from $59.99 to $79.99, said the U.S. Federal Trade Commission (FTC), which filed its own civil complaint against ClassicCloseouts.com and the owner in June 2009. When customers disputed the unauthorized charges with their credit card companies and banks, Classic Closeouts' owner asserted the charges were valid because the customers had enrolled in an alleged "frequent shopper club," the DOJ said. In some cases, customers were denied credit cards after the disputes or were pressured into paying the fraudulent charges, plus late fees and interest. The FTC announced a settlement with the owner in January, with the owner banned from owning Internet businesses that handle credit or debit accounts. The settlement also imposed a monetary judgment of nearly $2.1 million. It's uncommon for the DOJ to bring criminal charges after the FTC settles a civil case. The suspect faces a maximum sentence of 20 years in prison on the wire fraud charges. Source: http://www.pcworld.com/businesscenter/article/239452/internet_clothing_seller_charged_with_wire_fraud.html

New Zeus-based variant targets banks around the world. Another Zeus-based offering was unearthed September 5 by Trend Micros researchers, and experts surmised this one may be better crafted than the recently discovered Ice IX crimeware. Having analyzed the code, they believe it was created by using version 2.3.2.0. of the Zeus toolkit, and that it was created specifically for a professional gang. Experts note this solution is likely to succeed where Ice IX has failed: an updated encryption/decryption algorithm that should prevent trackers from analyzing its configuration file. Also, an update of the Zeus builder capability of checking for bot information and uninstalling it should make antivirus solutions unable to use it for detecting the bot and automatically purging the system of it. "It is also worth mentioning that this malware targets a wide selection of financial firms including those in the United States, Spain, Brazil, Germany, Belgium, France, Italy, Ireland, etc.," said the researchers. "More interestingly, it targets HSBC Hong Kong, which suggests that this new Zeus variant may be used in a global campaign, which may already include Asian countries." Source: http://www.net-security.org/malware_news.php?id=1828

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

New tool proposed for assessing chemical risks. The American Chemistry Council September 6 proposed a comprehensive, scientifically based system that could be used by the Environmental Protection Agency (EPA) to decide which chemicals require additional review and assessment, to help the agency update the Toxic Substances Control Act (TSCA). Now 35 years old, the TSCA does not dictate a process to use the information currently available to prioritize chemicals for review, the ACC noted. It said with no system in place, the EPA may be wasting time, energy, and resources gathering and analyzing data on chemicals that are already well understood or are unlikely to pose a significant risk to public health or the environment. The ACC's proposed system would evaluate chemicals against consistent scientific criteria that take into account hazard and exposure, giving each chemical a score based on the criteria and then ranking it based on the scores and EPA's best professional scientific judgment. The rankings would be

used to determine which chemicals are referred to EPA's Office of Chemical Safety & Pollution Prevention for further assessment. Before the proposal was announced, ACC representatives met with EPA officials to discuss the tool and how it could inform the agency's stakeholder dialogue on the TSCA update. Source: http://ohsonline.com/articles/2011/09/09/new-tool-proposed-for-assessing-chemical-risks.aspx?admgarea=news

UN watchdog says Libyan chemical weapons secure. Libya's remaining chemical weapon stockpiles are believed to be secure despite the turmoil that has roiled the country since February, the chief of a United Nations watchdog said September 7. The director general of the Organization for the Prohibition of Chemical Weapons said his inspectors are ready to return to Libya to oversee the destruction of poison gas supplies "when the conditions will allow us." He said he had heard from sources that "remaining stockpiles of chemical weapons are secured." In 2004, Libya's leader agreed to dismantle weapons of mass destruction, and he underscored his commitment by using bulldozers to crush 3,300 unloaded aerial bombs that could have been used to deliver chemical weapons. Libya destroyed nearly 15 tons of sulfur mustard in 2010, about 54 percent of its stockpile. It received an extension to eliminate the rest by May 15, the organization said. Nearly 40 percent of the chemicals used to make sulfur mustard also have been destroyed since 2005, it said. Twice-yearly inspections have found no evidence of Libya reviving the chemical weapons program. Source: http://www.boston.com/news/world/europe/articles/2011/09/07/un_watchdog_says_libyan_chemical_weapons_secure/

Commercial Facilities

(New York) **Coalition of groups plan to 'occupy Wall Street' on September 17, looking for an American Tahrir Square-moment.** A coalition of groups who said they've been inspired by the Arab Spring protests against despots abroad is calling for a large, Tahrir Square-like protest in New York City September 17. But what their demand will be is not yet clear. An online group dubbed "Occupy Wall Street" is calling for 20,000 people to "flood into lower Manhattan, set up tents, kitchens, peaceful barricades and occupy Wall Street for a few months," according to the Web site occupywallst.org. The site says "We also encourage the use of nonviolence to achieve our ends and maximize the safety of all participants." The original call to occupy Wall Street was put out by a group called Adbusters, which describes itself as a "global network of culture jammers and creatives working to change the way information flows, the ways corporations wield power, and the way meaning is produced in our society." The hacker/protest group Anonymous has also reportedly thrown its support behind the September 17 protest. Source: http://newyork.cbslocal.com/2011/09/06/groups-plan-to-occupy-wall-street-but-their-goal-is-not-yet-set/

(Tennessee) **Murfreesboro mosque receives bomb threat; feds investigate.** Murfreesboro, Tennessee police and DHS agents are investigating threats that someone plans to blow up the Islamic Center of Murfreesboro September 11. The threat was called in to the center about 1 a.m. September 5, and discovered the afternoon of September 6, said a Murfreesboro Police Department spokesman. The message said a bomb would be placed in the building September 11. The spokesman said there will be extra patrols around the Islamic center in the upcoming

days. Source: http://www.tennessean.com/article/20110907/NEWS03/309070087/Murfreesboro-mosque-receives-bomb-threat-feds-investigate

(Nevada) **4 dead, 6 wounded in Nevada shooting.** A man with an automatic rifle opened fire at an IHOP restaurant in Carson City, Nevada, September 6, killing two National Guard members, another person, and himself in a hail of gunfire during the morning breakfast hour, authorities and witnesses said. Six people were wounded in the attack. The suspect apparently acted alone and died at a hospital in Reno. Authorities were not saying whether the attack targeted the Guard members, who were meeting at the restaurant in a strip mall on Carson City's main street. Witnesses said the gunman pulled up in a blue minivan around 9 a.m. and shot a man on a motorcycle, then walked inside the restaurant and started shooting. He then walked outside and fired shots at a barbecue restaurant and an H&R Block in the strip mall, and then a casino across the street before turning the gun on himself. The state capitol and supreme court buildings were locked down for about 40 minutes, and extra security measures were put in place at state and military buildings in northern Nevada, but the shooting appeared to be an isolated incident, said the Carson City sheriff. Local, state police, and the FBI responded. The minivan was registered locally. A public relations manager for Care Flight told the Reno Gazette-Journal that three victims were taken to the hospital by helicopter, and that two were in critical condition. Source: http://today.msnbc.msn.com/id/44410882/ns/today-today_news/t/wounded-shooting-nevada-restaurant/

Communications Sector

(Washington) **Power surge that shut down Washington state government network to cost $500,000.** A power surge that shut down the State of Washington's internal network in August for several hours will end up costing the government $500,000, officials said September 6. The department of general administration (GA) estimates it will cost about $130,000 to purchase and install a new electrical vault switch. A contractor was working on a new high-voltage power line 2 weeks ago when equipment in the underground vault short-circuited. The ensuing power surge shut down electricity to the entire campus, and forced a hard shutdown of the state's data center. The data center hasn't been fully shut down in more than 20 years. A GA spokesman said officials are still working together to determine exactly what happened and how to prevent it from happening again. The outage occurred on a Sunday afternoon, and most services were up and running by the next day. The outage caused the largest problems at the employment security department, which had a delay processing unemployment claims. Source: http://www.therepublic.com/view/story/fe90889fb27e4582affd93912195027a/WA--Network-Shutdown/

Critical Manufacturing

McAfee report: vehicles exposed due to lack of security. McAfee released a study September 7 to raise the awareness of the automotive industry about the potential dangers behind the embedded devices used in most automobiles parts. Airbags, anti-lock braking systems,

electronic stability control, and autonomous cruise control are just a few of the components that could malfunction due to outside tampering, leading to potential injuries. The senior vice president and general manager of McAfee said that "[a]s more and more functions get embedded in the digital technology of automobiles, the threat of attack and malicious manipulation increases ... Many examples of research-based hacks show the potential threats and depth of compromise that expose the consumer," he stated. In the rush to add new car features such as Internet access, security has been overlooked, the report said. Source: http://news.softpedia.com/news/McAfee-Report-Vehicles-Exposed-Due-to-Lack-of-Security-220653.shtml

Honda recalls 962,000 cars worldwide. Honda Motor Company said September 5 it will recall 962,000 cars worldwide to fix power windows and computer systems. Honda will recall 936,000 units of the Fit subcompact, CR-V crossover, and Fit Aria in North America, Asia, Europe, and Africa, the company said. Honda said the recall was prompted by defects in driver's-side power window switch units that could potentially melt and catch fire. It will also recall 26,000 CR-Z compact hybrids globally due to programming problems with the engine control unit. There have been no injuries because of the defects, Honda said. Source: http://www.newser.com/story/127758/honda-recalls-962000-cars-worldwide.html

Defense/ Industry Base Sector

Former NASA, DOD scientist pleads guilty to attempted spying for Israel. A former government scientist who ran many highly classified projects for NASA, the Defense Department, and the Department of Energy pleaded guilty September 7 to attempted espionage for his efforts to sell classified information to Israel. The man, from Chevy Chase, Maryland, was arrested October 19, 2009, in Washington, D.C. by the FBI after he believed he was meeting with Israeli intelligence agents to pass information to them in exchange for money. The FBI began its investigation in 2002 when agents executed a search warrant at his home in a fraud investigation and discovered classified documents. The man, who established his own company, ACT, had been under criminal investigation by NASA's Office of the Inspector General for submitting false billing records to NASA and the Defense Department as part of his contracting work. According to court records, in January 2009, as he traveled overseas, a security check of his personal bags indicated he had two computer thumb drives. However, when he returned on his trip, the drives were no longer in his possession, according to the government. The FBI used an undercover agent to approach the man in September 2009, who told the man he worked for Israeli intelligence. During a lunch meeting with the agent, the man indicated he was willing to work for Israeli intelligence and provide them data. In the next several months, the FBI lured him into using "dead drops," where the man left envelopes with encrypted thumb drives with top secret information about key U.S. weapon and satellite systems in exchange for cash. Source: http://abcnews.go.com/blogs/headlines/2011/09/former-nasa-dod-scientist-pleads-guilty-to-attempted-spying-for-israel/

RSA spearphish attack may have hit U.S. defense organizations. Computerworld reported September 8 that the hackers who broke into EMC's RSA Security division last March used the same attack code to try to break into several other companies, including two U.S. national security organizations, according to data provided by the VirusTotal Web site. Before the attack was publicly disclosed in mid-March, the same maliciously encoded Excel spreadsheet involved in the RSA Security attack had been uploaded to the VirusTotal service's battery of antivirus checks 16 times from 15 different sources. The malware was detected by none of the site's 42 antivirus engines. The code was embedded in Excel documents, but the flaw it exploited when the documents were opened lay in Adobe's Flash Player. According to VirusTotal's founder, two of the targets were entities related to U.S. national security. The Contagio Malware Dump blog listed four different Excel files used in attacks, including a Nuclear Radiation Exposure And Vulnerability Matrix(dot)xls file that was doctored to look as though it came from the U.S. Nuclear Regulatory Commission. It's not clear who this file was sent to, but in the March 17 spearphishing e-mail also published on the blog, the attackers seemed to target people interested in the recent Japan earthquake. With the subject line, "Japan Nuclear Radiation Leakage and Vulnerability Analysis," the e-mail states, simply, "The team has poured in heart and full dedication into this. Would be grateful if you appreciate it." Source: http://www.computerworld.com/s/article/9219873/RSA_spearphish_attack_may_have_hit_U.S._defense_organizations?taxonomyId=13

Former L-3 employee indicted for allegedly exporting military tech. A former employee of defense contractor L-3 Communications Holdings Inc. was indicted September 7 for allegedly misappropriating and exporting sensitive military technology to China, the U.S. Department of Justice said. The indictment charges the man with eight counts of exporting defense-related technical data without a license, one count of transporting stolen goods across state lines, and two counts of making false statements to law enforcement agents. An earlier indictment filed in April against the man included one export-control charge, and two false-statements charges. The arraignment has been scheduled for September 14 in Newark, New Jersey federal court. The man was arrested in March at his residence by the FBI and DHS and was released on bond. According to the indictment, the man worked for L-3's space and navigation unit from March 2009 to November 2010 as a senior staff engineer. His team worked on navigation and positioning devices used in artillery and missile systems by the Department of Defense. After he returned from China, U.S. Customs and Border Protection officers in November 2010 found him in possession of a non-work-issued computer that was later found to contain numerous L-3 Communications documents relating to those systems. Source: http://www.google.com/url?sa=t&source=web&cd=1&ved=0CBsQqQIwAA&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FBT-CO-20110907-715091.html&rct=j&q=Former%20L-3%20employee%20indicted%20for%20allegedly%20exporting%20military%20tech&ei

Ex-employee wiped financial data from bikini bar. At the Bikinis Sports Bar and Grill in Austin, Texas, a recently fired IT worker broke into a U.S. military contractor's computer systems and wiped out payroll files, wreaking havoc on its customers January 21, 2010. Angry that his former employer, McLane Advanced Technologies, had fired him and then refused to help him with an unemployment benefits claim, the hacker broke into McLane's systems and deleted

payroll files belonging to Lone Star Plastics, a McLane customer that makes polyethylene bags and can-liners. He also broke into a second McLane customer, Capstone Mechanical. When employees at Lone Star Plastics' Prattville, Alabama-facility tried to punch in January 21, they discovered the McLane server that hosted their punch clock software and payroll records had shut down. Two days later, McLane contacted the U.S. Secret Service, reporting it was hacked. The hacker, formerly an IT administrator with the company, pleaded guilty to computer intrusion charges September 1 in U.S. District Court for the Western District of Texas. He is set to be sentenced November 2. Source: http://www.computerworld.com/s/article/9219721/Ex_employee_wiped_financial_data_from_bikini_bar

Emergency Services

(Texas) **Anonymous hack of Texas Police contains huge amount of private data.** Private data belonging to 26 Texas law enforcement agencies that was published online by the hacking group Anonymous earlier this month contains hundreds of Social Security numbers, scores of passwords, and loads of other sensitive data, according to a leading developer of data loss prevention software. Anonymous hackers released a 3GB file containing e-mails and documents from Texas law enforcement agencies September 2, claiming the data dump was done in retaliation for recent arrests of alleged members of the loosely affiliated hacking group. Identity Finder, a developer of identity protection and data loss prevention software, combed through the 3GB file with its DLP software tool, which analyzes files and e-mails to determine whether sensitive information exists in them. As with the earlier AntiSec breach, the Texas data dump contains a staggering amount of sensitive information, including passwords, street addresses, credit card numbers, personal identification numbers, and other information. Identity Finder broke down the particular of just what was published, which includes: 418 Social Security numbers; 26 credit card and bank account numbers; 83 drivers license numbers; 14,701 phone numbers; 4,631 personal postal addresses; 39,419 e-mail addresses. Source: http://www.pcmag.com/article2/0,2817,2392522,00.asp

DEA to ban so-called 'bath salts' drugs. Under mounting pressure from states, the federal Drug Enforcement Administration (DEA) said September 7 it will temporarily outlaw possession and sale of three synthetic stimulants — often marketed as "bath salts" — as dangerous chemicals that pose an imminent hazard to public health. A CBS News correspondent reported that at least 27 states have already banned the stimulants, and the DEA ban will take effect in 30 days. Sometimes packaged as bath salts or plant food and marketed under names such as "Purple Wave," "Vanilla Sky" and "Bliss," the stimulants are especially popular among teens and young adults and are perceived as mimics of cocaine, LSD, and methamphetamine. Bath salts are lab-produced stimulants called "synthetic cathinones" that mimic the effect of marijuana but are more powerful, and can cause users to hallucinate and become extremely violent. The DEA said users have reported disorientation, extreme paranoia and violent episodes after ingesting the chemicals. They are sold on the Internet and in head shops and other retail outlets. The ban will last at least a year, during which the government will determine whether it should permanently

control the stimulants — Mephedrone, MDPV, and Methylone. Source: http://www.cbsnews.com/stories/2011/09/07/national/main20103062.shtml

Report: Cell phone use by prisoners on the rise. Over the last 3 years, the number of contraband cell phones seized in federal prisons and minimum-security facilities has quadrupled, according to a report issued by the General Accountability Office. Corrections officials have been alarmed by the trend because prisoners can make unmonitored calls and can continue criminal activities while behind bars. The Bureau of Prisons needs to do a better job of evaluating technologies to detect the phones, the report said. In 2008, 1,774 cell phones were seized. By the end of 2010, that number had skyrocketed to 8,656. The study looked at the issue in federal prisons as well as institutions in eight states. The numbers were not complete for all the states, but in California, 900 phones were discovered in 2007, and 10,700 were found in 2010. When dangerous inmates had access to phones, the consequences often were grave. The report said in 2007, an inmate at a Maryland detention center ordered the murder of a witness to his crimes using a contraband phone. In another instance from 2008, a death row inmate in a Texas state prison used a cell phone to threaten a state senator and his family. Source: http://www.cnn.com/2011/CRIME/09/06/prisoners.cell.phones/index.html?hpt=ju_c2

ENERGY

(New York) **DEC releases hydrofracking report, will hold hearings.** The New York State Department of Environmental Conservation (DEC) will host four public hearings across the state and will lengthen a comment period on its latest review of hydraulic fracturing, the agency announced September 7. The hearings will be held in Broome, Steuben and Sullivan counties, as well as New York City, and will take place in November. The public will have 97 days to have its say on the DEC report, 37 days longer than originally planned. Environmental and conservation groups had been calling for 180 days to comment. The DEC also announced it will begin in October the process of developing the recommendations in its review into official regulations, which will require a separate comment period that will take place simultaneously. If approved, the rules would have the same force as state law. The agency posted a new draft of its 3-year review — dubbed the Supplemental Generic Environmental Impact Statement — September 6, weighing in at 1,537 pages. The draft has a new chapter on the economic and community impacts of natural gas drilling and hydrofracking, a controversial technique that involves the use of a mixture of water, sand and chemicals to break up shale formations — such as the Marcellus Shale — and release natural gas. Source: http://www.wgrz.com/news/article/133871/37/DEC-Releases-Hydrofracking-Report-Will-Hold-Hearings--

Evidence of infected SCADA systems washes up in support forums. A security researcher said evidence viruses and spyware have access to industrial control systems is hiding in plain sight: on Web based user support forums. Close to a dozen log files submitted to a sampling of online forums show evidence signs laptops and other systems used to connect to industrial control systems are infected with malware and trojans, including one system used to control machinery

for British-based energy firm Alstom UK, according to an industrial control systems expert. He said he uncovered almost a dozen log files from computers connected to industrial control systems while conducting research online. The configuration log files, captured by the free tool HijackThis by Trend Micro, were willingly submitted by the computer's operator to weed out malware infections. The random sampling suggests critical infrastructure providers are vulnerable to attacks that take advantage of mobile workers and contractors wo bring infected laptops and mobile devices into secure environments. The researcher circulated his findings via Twitter and discussed them in a blog post for Digital Bond, a consulting firm that specializes in work with firms in the control systems space. He discovered the links between infected Windows systems and industrial control systems by analyzing the HijackThis logs posted on the forums, which reveal detailed configuration information about the systems in question, the organization it belonged to, and even the role of the individual who owned the system. Source: http://threatpost.com/en_us/blogs/evidence-infected-scada-systems-washes-support-forums-090611

Food and Agriculture

(Oregon; Washington) **Harmful potato disease appears in Eastern Oregon.** Researchers in Oregon have discovered for the first time in Umatilla and Morrow counties a potentially devastating disease affecting potato crops. Plant pathologists confirmed September 2 the presence of zebra chip in five different potato varieties in the southern Columbia Basin. The affected varieties are Russet Ranger, Umatilla Russet, Pike, Alturas, and Russet Norkotah, which account for most of the acreage in the basin, said a U.S. Department of Agriculture plant pathologist. Source: http://www.eastoregonian.com/news/agriculture/harmful-potato-disease-appears-in-eastern-oregon/article_58edb72c-da3c-11e0-87bd-001cc4c03286.html

(New York; New Jersey; Connecticut) **Allergy alert: Raisins recalled for sulfites.** Best Food Cash & Carry Inc. of Maspeth, New York recalled 14-ounce packages of "Deer Raisin Golden" raisins because they contain undeclared sulfites. Consumers who have severe sensitivity to sulfites run the risk of serious or life-threatening allergic reactions. The problem was discovered after routine sampling by the New York State Department of Agriculture and Markets Food Inspector, and subsequent analysis by Food Laboratory personnel, the company said in a news release. The consumption of as little as 10 milligrams of sulfite per serving has been reported to elicit severe reactions in some asthmatics, including anaphylactic shock in some sensitive individuals. Analysis revealed the raisins contained 11.07 milligrams per serving. The presence of sulfites was not declared on any label. No illnesses have been reported to date. The recalled raisins were distributed in 14-ounce, clear, uncoded, plastic packages in New York, New Jersey, and Connecticut retail stores. Source: http://www.foodsafetynews.com/2011/09/allergy-alert-raisins-recalled-for-sulfites/

Costly cattle diseases found to have a genetic link. The origins of three costly cattle diseases are genetically linked, according to U.S. Department of Agriculture (USDA) researchers, the Kalamazoo Gazette reported September 8. A USDA news releas said scientists at the Agricultural Research Service have discovered the incidence of the most prevalent bacterial

diseases in feedlot cattle — pinkeye, foot rot, and pneumonia — is tied to a specific location on a specific bovine chromosome. Pneumonia in cattle accounts for 75 percent of feedlot illnesses and up to 70 percent of all deaths, with economic losses to cattle producers exceeding $1 billion annually, the agency said. The estimated costs for pinkeye amount to about $150 million yearly, and losses to dairy producers due to foot rot range from $120 to $350 per animal, according to the USDA. Results from the research were published in the Journal of Animal Science. Source: http://www.mlive.com/business/west-michigan/index.ssf/2011/09/costly_cattle_diseases_found_t.html

(Vermont) **Farmers obliged to plow under crops contaminated by flood water.** The Vermont Agency of Agriculture sent out an advisory September 2 telling farmers that any fruits or vegetables that came in contact with flood waters would have to be destroyed. The U.S. Food and Drug Administration said it is impossible to adequately clean produce after a field is flooded. And even though the state agriculture secretary knew the flooding occurred at one of the busiest times of the state's short growing season, he asked all farmers to abide by the directive to protect consumers. The agriculture agency said assistance will be available, and any farmers who suffered losses due to Tropical Storm Irene should contact their county farm services agency. The Vermont Economic Development Authority is also allocating up to $10 million in low interest loans to farms and businesses hurt by the floods. Vegetable farms tend to be located on rich, bottom lands, along rivers, and all across Vermont farmers are reported damage to crops, machinery, and fields. So far, an agriculture expert with University of Vermont Extension said losses are approaching $2 million, noting entire fields were washed away. But as bad as the flooding was for some, he said a majority of the farms in Vermont were spared the devastation, and there should be local produce available in the coming months. Source: http://www.benningtonbanner.com/local/ci_18831833

(Colorado) **Colorado officials: 2 dead, 7 sick in listeria outbreak.** State health department officials in Colorado are worried about a sudden listeria outbreak, and have renewed warnings about eating soft cheeses, meat spreads, undercooked hot dogs, and other potentially dangerous foods. Two people have died from the latest outbreak of the gastrointestinal illness that began in August. The department reported in June that two other people had died in a previous listeria outbreak, bringing the total of deaths this summer to four. The two August deaths came amid a rush of nine cases, compared to an average of two cases reported for the month in other years. Seven of the nine newest listeria illnesses have been reported since August 29. The "sharp increase" cited by Colorado officials deviates from an average of only 10 cases a year statewide. Patients were hospitalized in all nine recent cases of listeriosis, in the following counties: Adams, Arapahoe, Boulder, Denver, Douglas, El Paso, Jefferson, and Weld. Most of the patients were older and female, and ranged from their 30s to 90s. State investigators have not pinpointed the source or sources of the outbreak, and are continuing to research the eating habits and other health conditions of the patients. Source: http://www.denverpost.com/breakingnews/ci_18814105

Quaker Oats issues voluntary recall of specific 8-Count Quaker Chewy Smashbar Graham Pretzel snack bars due to undeclared milk allergen. Quaker Oats Company, a division of PepsiCo,

September 2 issued a voluntary recall of 8-count Quaker Chewy Smashbar Graham Pretzel snack bars due to an undeclared milk allergen not noted on the label. People who have an allergy or severe sensitivity to milk products run the risk of serious or life-threatening reactions if they consume this product. The affected product is limited to Quaker Chewy Smashbar Graham Pretzel snack bars with the UPC bar code ending in 31108 and best before dates: October 29 11 RB, October 30 11 MM, October 30 11 RB, Novenber 22 11 RB, November 23 11 RB, November 24 11 RB, November 27 11 RB, December 22 11 RB, December 22 11 MM, December 23 11 RB, December 23 11 MM, December 24 11 RB, December 24 11 MM stamped on the side of the package. Consumers with a milk allergy who have this product should return it to the retailer where it was purchased for a full refund. One allergic reaction had been reported as of September 2. Source: http://www.sacbee.com/2011/09/02/3881409/quaker-oats-issues-voluntary-recall.html

(Virginia) **Hurricane Irene damages cotton, corn crops.** Corn and cotton bore the brunt of Hurricane Irene's wrath August 27, making up most of the more than $9 million in estimated crop losses and damages reported by growers in rural Peninsula and Western Tidewater counties of Virginia. Cotton, which hit historically high prices earlier this year, is now a mangled, flattened mess in many fields across Isle of Wight and Surry counties. Irene's fierce winds also flattened acres of corn across southeastern Virginia. "It's devastating," said the secretary of agriculture and rorestry. He and other state officials visited the hardest hit sites September 2. Based on preliminary reports, the secretary estimated Virginia's agriculture industry took a $60 million or larger hit from Hurricane Irene. While most of the losses were corn crops, nursery plants, soybeans, and some row vegetables also sustained minor damage. Source: http://www.dailypress.com/news/isle-of-wight-county/dp-nws-cp-irene-farm-losses-0903-20110906,0,2775115.story

Raw milk mixed with pasteurized milk causes recall. An Illinois dairy recalled milk, cheese, and dairy products September 6 after the state health department found its pasteurizing equipment was not operating properly, potentially allowing raw milk to be mixed with pasteurized milk. State inspectors said a system-controlled pump, designed to stop the production process if raw milk pressure exceeded pasteurized pressure, was bypassed and replaced with a pump not wired into the controls at Ludwig Dairy Products, located in Dixon. As a result, Ludwig has recalled its name brand products, which are sold mostly in northern Illinois counties (Cook, DuPage, Kane, Lake, McHenry, Will), but also in Indiana, New Jersey, and New York. A drinkable yogurt product is also sold under the Nuestro Queso brand. In a news release, the Illinois Department of Health warned the public not to consume Ludwig products until the dairy pasteurizing equipment is operating correctly. People who have purchased the dairy products should throw them out, the state advised. Source: http://www.foodsafetynews.com/2011/09/raw-milk-mixed-with-pasteurized-milk-prompts-recall/

Government Sector (including Schools and Universities)

(California) **Navy corpsman linked to bomb threat surrenders.** An AWOL U.S. Navy corpsman turned himself in September 7 after leaving a threatening note claiming he planted bombs at a Southern California high school in an incident that prompted administrators to order students out of the building on the first day of classes in San Clemente, California. The Navy corpsman, 22, surrendered at Camp Pendleton Marine Corps base at around 1 p.m. September 7, a Master Sergeant said. The corpsman wrote he had placed explosive devices in and around San Clemente High School, which is located just a few miles from one of the gates to Camp Pendleton. Soon after the note was found, about 3,200 students and 180 faculty members were told to leave. They waited on the football field — and later in the gymnasium, auditorium, and other rooms — as bomb squads searched. After about 4 hours, everyone was sent home. Later September 7, a Marine spokesman said no military-grade explosives were missing from the base. A sheriff's lieutenant said no explosives or suspicious devices were found at the school during a five and a half hour search.Source: http://www.timesunion.com/news/article/AWOL-Navy-medic-linked-to-bomb-threat-surrenders-2159579.php

(Virginia) **Bomb threat closes Prince William County courthouse.** The Prince William County courthouse in Mananas, Virginia on Lee Avenue was closed for the day September 6 after someone called in a bomb threat from a pay phone in Woodbridge, Virginia police said. The courthouse was evacuated and traffic on Va. 28 between Grant Avenue and Stonewall Road was rerouted after the threat, which came in just before 2 p.m. Bomb sniffing dogs were checking the building and cars leaving the lot late the afternoon of September 6, said the Prince William County police spokesman. Some school buses were rerouted due to road closures, but city schools did not release students early. Criminal court cases were rescheduled for September 7. Source: http://www2.insidenova.com/news/2011/sep/06/2/bomb-threat-closes-prince-william-county-courthous-ar-1289310/

Fraudsters exploit leaked dot-mil addresses. A July leak of 90,000 military e-mail addresses and passwords has helped swindlers commit online fraud, FBI officials said. The hacktivist group Anonymous July 11 announced it had obtained, and later posted, the confidential data by cracking a computer system at defense contractor Booz Allen Hamilton. Now, imposters are using the traditionally trustworthy dot-mil addresses to place sham orders with e-commerce vendors, warned the Internet Crime Complaint Center, an FBI-led public private partnership. Businesses have witnessed an increase in fake dot-mil orders during the past 30 days, the center said September 1. "As a result of this posting, merchants have reported some orders containing military email addresses have been identified as fraudulent," stated a center advisory. "Until this time, military email addresses typically meant an order was less likely to be fraudulent." Source: http://www.nextgov.com/nextgov/ng_20110902_1237.php

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Cybercrooks aiming to cash in on 9/11 anniversary. Cybercrooks are preparing to commemorate the 10th anniversary of the September 11th attacks with a range of malware traps and hacking attempts on social networks and the wider Internet, net security firm BitDefender warned. The first wave of these attacks comes in the form of the newly established Web sites offering supposed content such as "Bin Laden alive," "in depth details about the terrorist attack," "police investigation results," and "towers going down" to attract the curious. The sites are filed with links to scareware and phishing sites. Others have created fraudulent charity donation sites. In addition, fraudsters are running fake auctions and sales of items supposedly linked to the attacks such as shards of metal from the twin tower or even "commemorative coins" supposedly minted from silver collected at the attack site. Source: http://www.theregister.co.uk/2011/09/08/9_11_anniversary_scams/

New trojan masquerades as Microsoft enforcement-ware. Malware-makers have created a strain of ransomware trojan that masquerades as a Microsoft utility. The Ransom-AN trojan claims a user's Windows machine is running an unlicensed copy of Windows, and threatens to cripple the computer unless $143 is paid to obtain an unlock code, which can be purchased via credit card via a scam Web site. The malware attempts to spook intended victims with entirely bogus claims that a criminal prosecution will be launched unless payment is received within 48 hours. In addition, the trojan says all data and applications on targeted systems will be "permanently lost." The malware, which targets German-speaking users, is being distributed via spam and P2P downloads. Panda Software, the net security firm which detected the threat, warned the trojan is difficult to remove manually. Source: http://www.theregister.co.uk/2011/09/07/ms_ruse_ransomware_trojan/

Phishers use new tricks. Internet users are becoming more aware of the dangers of phishing. As a result, phishers are implementing new methods of luring unsuspecting people into their nets. The latest "phishing expedition" was observed by Symantec. The malicious site was masked as a software company that offered considerable discounts. Users were then led to a page where they would be required to give out all their personal information, including credit card details, which would later be used to gain control of the person's financial records. Many people were drawn to the page by the up to 80 percent savings they could make on the site's main page. Researchers indicated the page containing the offers was hosted on a newly registered domain that ranked high in most of the popular search engines. This was achieved by using keywords in the domain name that are very common in related searches. The people behind this practice managed to make fake trust seals. The seals seemed legitimate because of some sub-domain randomization techniques used by the phishers. Source: http://news.softpedia.com/news/Phishers-Use-New-Tricks-220334.shtml

Incognito exploit kit discovered after Web Directories attack. Users who visited the Web Directories site September 4 may have been redirected to a third party page leveraging the Incognito exploit kit. One of the largest directories on the Internet, the site was compromised after a program line, representing a redirect to a malicious address containing exploit codes,

was inserted. An analysis made by Websense Security Labs revealed the hacking tool involved is known as Incognito, which silently infects the client computers with a trojan. According to the Security Labs blog, Incognito is a Malware as a Service (MaaS) which has two versions running in the wild. Underground communities use it to launch automated attacks with the purpose of spreading malware. Source: http://news.softpedia.com/news/Web-Directories-Site-Attacked-220361.shtml

National Monuments and Icons

(Texas) **Wildfire destroys nearly 500 homes in Texas.** Calmer winds September 6 were expected to help firefighters battling a wildfire that has destroyed nearly 500 homes in Central Texas, and forced thousands of residents to evacuate to shelters to avoid the blaze, officials said. At least 5,000 people were forced from their homes in Bastrop County about 25 miles east of Austin, and about 400 were in emergency shelters, officials said September 5. School and school-related activities were canceled September 6. The fire enveloped at least 25,000 acres September 5. There were no immediate reports of injuries, and officials said they knew of no residents trapped in their homes. Source: http://news.yahoo.com/wildfire-destroys-nearly-500-homes-texas-221031244.html

Postal and Shipping

(Illinois) **Suspicious items found in Illinois post office.** A postal worker in suburban Chicago said he discovered what looked like a half-stick of dynamite, a bullet and white powder in a broken envelope September 3. The Lyons, Illinois post office worker told the Chicago Tribune he was worried because the powder leaked onto his hands. Fire officials in Lyons said they responded to a call about a suspicious package. They treated the call as a hazardous materials incident. The postal worker said the post office was evacuated, and he and a female co-worker who came in contact with the powder were separated from other workers. Paramedics told the postal employee his vital signs were OK. He said the envelope did not have a return address. Source: http://www.sj-r.com/breaking/x1638742346/Suspicious-items-found-in-Illinois-post-office

Public Health

91 charged in $295M Medicare fraud crackdown. A nationwide law enforcement crackdown has charged 91 people, including doctors and other medical professionals, with participating in Medicare fraud schemes involving $295 million in false billing. Charges were filed in Baton Rouge, Louisiana; Brooklyn, New York; Chicago; Dallas and Houston; Detroit; Los Angeles; and Miami. Eleven of the people charged were doctors, three were nurses, and 10 were licensed health professionals. Forty-six defendants and $160 million of the total claims came from South Florida. In Miami, a U.S. attorney said investigators noticed people who were already receiving Medicare disability checks were recruited with promises they could live in a halfway house in South Florida as long as they agreed to receive mental health services they did not need. Many were addicted to drugs or alcohol, and some were homeless, and they would be threatened

with eviction if they did not participate in the fraud scheme. That particular scheme and other frauds, operated out of an entity called Biscayne Milieu, accounted for $50 million of the fraudulent Medicare claims, prosecutors said. It provided no legitimate services. In Houston, two people were charged with fraud schemes involving $62 million in false claims for home health care and medical equipment. One defendant allegedly sold beneficiary information to 100 Houston-area home health care agencies. The home agencies used the information to bill Medicare for services that were unnecessary or never provided. In Baton Rouge, a doctor, nurse, and five other co-conspirators were charged with billing Medicare more than $19 million for skilled nursing and other home health services that were not necessary or never provided. Source: http://news.yahoo.com/91-charged-295m-medicare-fraud-crackdown-042537318.html

A tick-borne parasite invades the blood supply. A parasitic infection normally transmitted by deer ticks has made its way into the U.S. blood supply, researchers from the U.S. Centers for Disease Control and Prevention (CDC) reported September 6. The infection is called babesiosis, and it is increasingly spreading through blood transfusions. The first case of babesiosis transmitted through transfusion occurred in 1979, according to the CDC. Since then, another 161 cases have been documented — 77 percent of them in the last decade. All but three of the cases recorded by the CDC were caused by the Babesia microti parasite. Although a history of babesiosis prohibits blood donation, many potential donors do not know they have been infected because the symptoms of babesiosis can be mild or nonexistent. And while doctors can run tests that detect the parasite or antibodies to it in the blood if an infection is suspected, there are currently no approved screens being used routinely for potential blood donors. The disease is treatable with antibiotics, but it can become severe or even deadly in certain vulnerable populations, including the elderly, those with weakened immune systems, and patients who do not have a spleen. Source: http://healthland.time.com/2011/09/07/a-tick-borne-parasite-threatens-the-blood-supply/

Transportation

Sheriffs: Tall corn creates hazard on rural roads. Tall stalks obstructing drivers' views are a fall hazard in the Corn Belt, but the danger could be greater as farmers seek to cash in on higher prices by expanding their fields closer to the edge of roads. With corn commanding twice what it did in 2011, farmers from Pennsylvania to the Dakotas have tried to plant as much as possible. The federal government has estimated planting at 92.2 million acres, up 5 percent from in 2010. In some cases, farmers have planted right up to the gravel in remote areas, a practice that can have deadly consequences at unmarked intersections. A Nebraska man was killed the week of August 29 when a pickup truck struck the four-wheeler he was driving on a road near his home. Officials in Iowa, the top corn-growing state, said they were concerned about visibility. Twenty-eight people have died since 2001 at rural intersections where vision was obstructed, according to the Iowa Department of Transportation (IDOT). The department's data does not differentiate between tall corn and other vegetation, but an IDOT spokesman said the crashes tend to occur in the late summer and early fall when corn is high. Source: http://news.yahoo.com/sheriffs-tall-corn-creates-hazard-rural-roads-070303962.html

(Iowa; Missouri; Nebraska) **Some state highways still submerged.** In Iowa, Missouri River floodwaters still cover sections of Interstate 29, U.S. Highway 30, and Iowa Highway 175 even though the river is receding as the U.S. Army Corps of Engineers ratchets down releases from Gavins Point Dam. The Corps expects river flows to return to normal by early October, but state transportation officials do not know when roads will reopen. Miles of pavement must be evaluated for safety and to determine if repairs are needed. Most of the problems remain in southern Iowa, from Missouri Valley south to the Missouri border, a spokeswoman for the Iowa Department of Transportation (IDOT) said September 6. Detours are posted. The IDOT has removed much debris from highways in Fremont and Pottawattamie counties, but crews have not been able to remove debris from ditches that remain filled with water. Areas still covered by floodwaters or closed due to flood damage include: I-29 from Council Bluffs north to milepost 71; I-29 from the Missouri state line to exit 32; I-680 from Council Bluffs to Omaha; U.S. Highway 30 west of Missouri Valley; Iowa 175 bridge to Decatur, Nebraska; and Iowa Highway 2. Regarding the Decatur bridge, the spokeswoman said preliminary inspections reveal the river channel has deepened around the bridge pier by 42 feet, with serious scouring and loss of embankment near the bridge abutment on the Iowa side. The IDOT is working with the Burt County (Nebraska) Bridge Commission and the Nebraska Department of Roads to finalize reconstruction plans. Source: http://www.siouxcityjournal.com/news/state-and-regional/iowa/article_395056f2-abb1-5d53-b4ec-709bb2f6f400.html

Amtrak restoring service to South destinations. Amtrak said it is beginning to resume operations to destinations in the South after disruptions by flooding from Tropical Storm Lee. Amtrak said in a news release that service would resume September 5 between New York and New Orleans, and between Chicago and New Orleans. Amtrak will resume full service between Los Angeles and New Orleans September 6. Amtrak warned there could be some delays due to rain. Amtrak said passengers who paid for travel on canceled trains can contact the company for refunds or can rebook for future travel. Source: http://www.chron.com/news/article/Amtrak-restoring-service-to-South-destinations-2156324.php

(Washington) **Man subdued after rushing jet exit door in Seattle.** A 39-year-old man is in custody after he tried to rush the exit door of an Alaska Airlines jet as it was taxiing to a gate at Seattle-Tacoma International Airport in Washington. An airport spokesman said passengers and the crew had to subdue the man September 5, who was apparently anxious to get off the plane. One crew member was bitten in the arm during the scuffle and was taken to Highline Medical Center in Burien, for treatment of minor injuries. The man was taken to Highline for a mental health evaluation, before being transferred to King County Jail. He was expected to be booked on investigation of felony assault. Flight 108 from Anchorage, Alaska, landed in Seattle at about 4:30 a.m. Source: http://news.yahoo.com/man-subdued-rushing-jet-exit-door-seattle-163200886.html

Winter threatens repairs of Irene-damaged roads. Northeastern states struggling to rebuild hundreds of roads and dozens of bridges in the wake of Hurricane Irene are facing another natural threat: winter. The end of construction season is fast approaching in New England, and

upstate New York. By November, it will be too cold to lay asphalt, and by December, snow and ice will cover the mountains, leaving towns dangerously isolated and possibly dissuading tourists during the region's ski season. Vermont officials said September 5 they are renting quickly built, military-style temporary bridges as a stopgap measure. Raging floods gouged and closed more than 300 local roads and state routes in Vermont, and damaged at least 22 bridges in the state, marooning people for days in at least 13 towns. Irene ripped another 150 roads in New York. Some of the washed-out roads have gaping gullies 30-feet deep. Road building experts said if the work is not done by mid-November, winter's cold, ice and snows will prevent any substantial progress until after the spring thaws. The consequences could be serious: residents forced to make 30-mile detours — on mountain roads, some unpaved — to the nearest grocery store or doctor, businesses struggling for customers, and a possible hit to winter tourism. Other states wrestling with post-Irene road repairs include New Hampshire, New Jersey, North Carolina, and Virginia. Vermont is negotiating leases and rent-to-own contracts with three companies to bring in military-style "Bailey bridges," a spokesman said. The bridges, made up of 10-foot sections of metal decking, may have to serve for 4 or 5 years until the state can finish permanent repairs, he said. Source: http://news.yahoo.com/winter-threatens-repairs-irene-damaged-roads-163528880.html

U.S. tanker trucks need anti-rollover retrofits, NTSB says. The National Transportation Safety Board (NTSB) urged regulators to require rollover-prevention technology on fuel-tanker trucks, following its probe of a fiery 2009 crash in Indianapolis. The Federal Motor Carrier Safety Administration, the Transportation Department's trucking regulator, should mandate anti-rollover retrofits for cargo tank trailers that weigh more than 10,000 pounds, the NTSB said in recommendations sent September 1. Tankers carrying hazardous materials may be top-heavy and vulnerable to minor steering errors, the board said in its accident report. Quality Distribution Inc. and Groendyke Transport are among the companies that would be affected by a retrofit. The NTSB, which cannot implement changes, completed its investigation of the crash in July, concluding a rollover that released 9,001 gallons of liquefied petroleum gas could have been prevented with stability control. Without regulation, the trucking industry has had little incentive to pay for the technology, the board said. Because of the long working life of tankers, it may take 50 years for stability control technology to be used throughout fleets without mandated retrofits, it said. The October 22, 2009 crash displaced a pier holding a bridge on Interstate 465, closing an interchange for several days. The trucker and another driver sustained serious injuries. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/09/01/bloomberg1376-LQWIJJ6JIJUT01-6OISFH83ESPR2OUDRK5IL90902.DTL

Water and Dams

Sewage-tainted floodwaters threaten public health. Floodwaters from the remnants of storms Lee and Irene — tainted with sewage and other toxins — threaten public health in parts of the Northeast by direct exposure or the contamination of private water wells, officials said September 9. A dozen Vermont towns flooded by Irene were still on boil-water orders 12 days later, though officials reported no water-borne illness. Similar precautions have been taken

throughout other storm-damaged states. In Waterbury, Connecticut, the municipal wastewater plant was overwhelmed by flooding from Irene, and raw sewage flowed into the Winooski River. On September 7, the Vermont Agency of Natural Resources said septic tanks continued to be a threat since the storm hit August 28. New York City officials said any threat from Irene's backwash had passed, but upstate, 23 municipal water systems had boil-water orders for varying lengths of time. As some communities in New Jersey and Pennsylvania were taking similar precautions after Irene, the unrelenting rains of Lee were expected to trigger more. Officials in Maryland, Delaware, and the District of Columbia, which were also hit hard by Irene, said drinking-water quality had not been compromised. In addition to concerns about water-borne illness, residents of affected areas were being urged to avoid exposure to water and mud possibly polluted with household chemicals and paints. Source: http://www.ajc.com/news/nation-world/sewage-tainted-floodwaters-threaten-1164721.html

(Florida) **Saltwater imperils South Florida's drinking water supply.** Many cities along South Florida's coast are running out of water as drinking wells are taken over by the sea, the Miami Herald reported September 4. Hallandale Beach in south Florida abandoned six of its eight drinking water wells because saltwater advanced underground across two-thirds of the city. "The saltwater line is moving west and there's very little that can be done about it," said a city commissioner for Hallandale Beach. A wall of saltwater is inching inland into the Biscayne Aquifer — the primary source of drinking water for 4.5 million people in South Florida. A city commissioner and Hallandale Beach city staff are looking to secure a new source of drinking water. The project will cost an estimated $10 million, said the deputy director of Hallandale Beach Utilities and Engineering. Residents will eventually pay those capital costs. New drinking water wells are likely the cheapest alternative, the commissioner said. The city could build a reverse osmosis plant to filter out the salt, but the construction and maintenance costs would be very high. Source: http://www.sacbee.com/2011/09/04/3884858/saltwater-imperils-south-floridas.html

(Maine) **Arsenic in Maine: threat from below.** The Kennebec Journal reported September 4 that a U.S. Geological Survey study released in 2010 showed, using data from more than 11,000 wells in 530 Maine communities, three high-arsenic clusters in the state: the southern coast, Down East, and Greater Augusta. Gorham and Scarborough are 2 of the 10 Maine communities showing the highest concentrations of arsenic in private well water, and 5 of the 10 are found in Kennebec County. A Columbia University study estimated 31 percent of private wells in Greater Augusta contain arsenic levels above the federal standard. Using various analytical methods, Columbia researchers found 12,293 to 15,561 Kennebec County residents are drinking from private wells containing toxic levels of arsenic, which has been linked to increased risk of skin, lung, and bladder cancer; developmental problems in children; diabetes; and immune system disorders. The problem — naturally occurring arsenic seeping from underlying rock — is particularly prevalent in Readfield and Manchester, and in a band along the western edge of the county from Winthrop and Monmouth south through Hallowell and Litchfield. Maine does not require any testing of private wells, on which 74 percent of Kennebec County homes rely for potable water, according to U.S. Census data. Source: http://www.pressherald.com/news/arsenic-in-maine-threat-from-below_2011-09-04.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168